Cybersecurity Act

Information on the Cybersecurity Act

Last updated 2 April 2025

The Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Amendments to the Act was passed in Parliament in May 2024.

The key objectives of the Cybersecurity Act are to:

1. Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks

CII are computer systems directly involved in the provision of essential services. Cyber-attacks on CII can have a debilitating impact on the economy and society. The Act provides a framework for the designation of CII, and provides CII owners with clarity on their obligations to proactively protect the CII from cyber-attacks. This builds resilience into the CII, protecting Singapore's economy and our way of life. The CII sectors are: Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Infocomm, Media, Security and Emergency Services, and Government.

2. Authorise CSA to prevent and respond to cybersecurity threats and incidents

The Act empowers the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents to determine their impact and prevent further harm or cybersecurity incidents from arising. The powers that may be exercised are calibrated according to the severity of the cybersecurity threat or incident and measures required for response. This assures Singaporeans that the Government can respond effectively to cybersecurity threats and keep Singapore and Singaporeans safe.

3. Establish a framework for sharing cybersecurity information

The Act also facilitates information sharing, which is critical as timely information helps the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request information, and for the protection and sharing of such information.

4. Establish a licensing framework for cybersecurity service providers

CSA adopts a light-touch approach to license only two types of service providers currently, namely penetration testing and managed security operations centre (SOC) monitoring. These two services are prioritised because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in our market and hence have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cybersecurity ecosystem.

Amendments were made to update the Act so that it keeps pace with the developments in the cyber threat landscape, as well as our evolving technological operating context.

The key amendments include:

1. **Update of existing provisions relating to cybersecurity of CII**. The Act has been amended to ensure that CII owners remain responsible for the cybersecurity and cyber resilience of the CII, even as they embrace new technological and business models, like the use of cloud computing. CII owners will also be required to report more types of incidents, such as those that happen in their supply chains. This will ensure better situational awareness of cybersecurity threats for CSA to work with CII owners more proactively to secure our essential service.

2. **Expansion of CSA's oversight to cover new classes of regulated entities.** Given the evolving digital landscape, the Act allows CSA to proactively secure Systems of Temporary Cybersecurity Concern (STCCs), i.e. computer systems that are of higher risk due to temporary events or situations. In addition, the Act allows CSA to designate and regulate Entities of Special Cybersecurity Interest (ESCI) for cybersecurity if they hold sensitive information or perform a function of national interest. Finally, companies that provide digital infrastructure services that are foundational to our economy or way of life (such as cloud service providers and data centres) will be regulated as Foundational Digital Infrastructure (FDI) and they are required to adhere to cybersecurity codes and standards of practice, as well as reporting prescribed cybersecurity incidents.

You can access the related sources:

1. Cybersecurity Act ↗ on Singapore Statutes Online
2. For the Explanatory Statement of the Cybersecurity Act [PDF, 197 KB] ↗
3. Cybersecurity (Amendment) Bill and Explanatory Statement ↗
4. Opening speech to Second Reading of Cybersecurity (Amendment) Bill by SMS Janil Puthucheary
5. Closing speech to Second Reading of Cybersecurity (Amendment) Bill by SMS Janil Puthucheary
6. Infographic on key changes in Cybersecurity (Amendment) Bill [PDF, 1.3 MB] ↗

For FAQs, please click here.